No. 19-1435

IN THE

Supreme Court of the United States

LAURA TANNER,

Petitioner,

v.

STATE OF AMES,

Respondent.

ON WRIT OF CERTIORARI TO THE
SUPREME COURT OF THE STATE OF AMES

BRIEF FOR RESPONDENT

The Lloyd L. Gaines Memorial Team

JASON BELL
AMEZE BELO-OSAGIE
LAUREN BILOW
DAVIS CAMPBELL
TRAVIS FIFE
MICHAEL TORCELLO

Counsel for Respondent

MARCH 10, 2021, 7:30 PM
AMES COURTROOM
HARVARD LAW SCHOOL

Oral Argument

QUESTIONS PRESENTED

1. Whether the Ames Nonconsensual Pornography Act, Ames Crim. Stat. 545, violates the First Amendment.

2. Whether the Fifth Amendment privilege against self-incrimination allows a defendant to refuse to disclose the password to her computer and phone when the government has a warrant to search those devices.

TABLE OF CONTENTS

QUESTIONS PRESENTED i

TABLE OF CONTENTS ii

TABLE OF AUTHORITIES iv

OPINIONS BELOW 1

JURISDICTIONAL STATEMENT 1

RELEVANT PROVISIONS 1

STATEMENT OF THE CASE 2

SUMMARY OF THE ARGUMENT 7

ARGUMENT 10

I. The NCPA does not violate the First Amendment 10

A. The First Amendment does not protect nonconsensual pornography 11

1. Nonconsensual pornography is obscene 11

2. Nonconsensual pornography should be identified as a new categorical exception to First Amendment protection 13

a. History supports a categorical exception for nonconsensual pornography 13

b. First Amendment values support a categorical exception for nonconsensual pornography 15

B. The NCPA withstands intermediate scrutiny 17

C. The NCPA withstands strict scrutiny 22

1. Nonconsensual pornography threatens the State's compelling interests in citizens' welfare and privacy 23

2. The NCPA is narrowly tailored to advance the State's compelling interests 24

3. The NCPA is the least restrictive means of advancing the State's interests 28

D. The NCPA is not overbroad 30

E. This Court should sever any portions of the NCPA that it deems invalid 32

II. Compelled password disclosure does not violate the Fifth Amendment 33

A. Compelled password disclosure is not incriminating 34

1. A password is not incriminating because it is a sequence of characters with no evidentiary value..... 35

2. Petitioner's purely causal theory of incrimination is inconsistent with this Court's precedents..... 36

3. Both Petitioner's purely causal theory and her conclusion that password disclosure is incriminating are inconsistent with the original understanding of the privilege..... 39

4. Even if Petitioner's purely causal theory of incrimination found support in this Court's precedents, it should not apply in this case..... 42

B. Compelled password disclosure is insufficiently testimonial to warrant application of the privilege..... 44

C. Compelled password disclosure is permitted under the foregone conclusion exception because the disclosure would not meaningfully add to the State's knowledge 48

D. Petitioner's argument that the Fifth Amendment categorically bars compelled production of private documents is immaterial to this case 51

1. Petitioner's argument is outside the scope of the question presented 51

2. Petitioner's proposed rule does not support reversal of the judgment below..... 53

CONCLUSION..... 55

APPENDIX..... A-1

U.S. Const. amend. I A-1

U.S. Const. amend. V A-1

Nonconsensual Pornography Act, Ames Crim. Stat. 545 .... A-1

Sup. Ct. R. 14..... A-3

TABLE OF AUTHORITIES

Cases

Ashcroft v. ACLU,
535 U.S. 564 (2002) 12

Ashcroft v. Free Speech Coal.,
535 U.S. 234 (2002) 17

Ayotte v. Planned Parenthood of N. New Eng.,
546 U.S. 320 (2006) 32

Bartnicki v. Vopper,
532 U.S. 514 (2001) 23

Brigham City v. Stuart,
547 U.S. 398 (2006) 44

Broadrick v. Oklahoma,
413 U.S. 601 (1973) 30, 31

Brockett v. Spokane Arcades, Inc.,
472 U.S. 491 (1985) 32

Carpenter v. United States,
138 S. Ct. 2206 (2018) 42, 54

Cent. Va. Cmty. Coll. v. Katz,
546 U.S. 356 (2006) 48

Chaplinsky v. New Hampshire,
315 U.S. 568 (1942) 10

City of Renton v. Playtime Theatres, Inc.,
475 U.S. 41 (1986) 18, 19

Davenport v. Wash. Educ. Ass'n,
551 U.S. 177 (2007) 18, 19

Doe v. United States (*Doe II*),
487 U.S. 201 (1988) ..... *passim*

Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.,
472 U.S. 749 (1985) 21

Fisher v. United States,
425 U.S. 391 (1976) ..... *passim*

Folsom v. Marsh,
9 F. Cas. 342 (C.C.D. Mass. 1841) (No. 4,901) 14

Gee v. Pritchard
(1818) 36 Eng. Rep. 670 14

Gilbert v. California,
388 U.S. 263 (1967) 46

Ginzburg v. United States,
383 U.S. 463 (1966) 12

Griswold v. Connecticut,
381 U.S. 479 (1965) 23

Hamling v. United States,
418 U.S. 87 (1974) 26

Hiibel v. Sixth Jud. Dist. Ct.,
542 U.S. 177 (2004) 34, 36, 43

Hoffman v. United States,
341 U.S. 479 (1951) 34, 36, 37

Holder v. Humanitarian L. Project,
561 U.S. 1 (2010) 30

In re Harris,
221 U.S. 274 (1911) 49

Izumi Seimitsu Kogyo Kabushiki Kaisha v. U.S. Philips Corp.,
510 U.S. 27 (1993) 52

Kastigar v. United States,
406 U.S. 441 (1972) 34, 37

King v. Purnell
(1748) 96 Eng. Rep. 20 53

Lawrence v. Texas,
539 U.S. 558 (2003) 23

Members of the City Council v. Taxpayers for Vincent,
466 U.S. 789 (1984) 19

Miller v. California,
413 U.S. 15 (1973) 11, 15

Miranda v. Arizona,
384 U.S. 436 (1966) 44

Murphy v. Waterfront Comm'n,
378 U.S. 52 (1964) 39, 43

N.Y. State Club Ass'n v. City of New York,
487 U.S. 1 (1988) 31

N.Y. Times Co. v. Sullivan,
376 U.S. 254 (1964) 29

New York v. Ferber,
458 U.S. 747 (1982) 17, 26, 28, 33

O'Connor v. Ortega,
480 U.S. 709 (1987) 25

Paris Adult Theatre I v. Slaton,
413 U.S. 49 (1973) 12

Pennsylvania v. Muniz,
496 U.S. 582 (1990) 46

People v. Austin,
155 N.E.3d 439 (Ill. 2019), *cert. denied*,
141 S. Ct. 233 (2020) (mem.) ..... *passim*

Perma Life Mufflers, Inc. v. Int'l Parts Corp.,
392 U.S. 134 (1968) 17

Poe v. Ullman,
367 U.S. 497 (1961) 2

R.A.V. v. City of St. Paul,
505 U.S. 377 (1992) 18, 19

Reed v. Town of Gilbert,
576 U.S. 155 (2015) 18, 19, 20, 22

Reno v. ACLU,
521 U.S. 844 (1997) 28

Riley v. California,
573 U.S. 373 (2014) 42, 43, 54

Roe v. Harvey
(1769) 98 Eng. Rep. 302 53

Shalala v. Ill. Council on Long Term Care, Inc.,
529 U.S. 1 (2000) 20

Snyder v. Phelps,
562 U.S. 443 (2011) 21

Splawn v. California,
431 U.S. 595 (1977) 12

State v. Andrews,
234 A.3d 1254 (N.J. 2020) 35, 49, 53

State v. Casillas,
952 N.W.2d 629 (Minn. 2020) 23, 28

State v. Stahl,
206 So. 3d 124 (Fla. Dist. Ct. App. 2016) 49

State v. VanBuren,
214 A.3d 791 (Vt. 2019) ..... *passim*

Sweatt v. Painter,
339 U.S. 629 (1950) 53

Terminiello v. City of Chicago,
337 U.S. 1 (1949) 2

Trump v. Vance,
140 S. Ct. 2412 (2020) 33

Turner Broad. Sys., Inc. v. FCC,
512 U.S. 622 (1994) 18

Union Pac. Ry. Co. v. Botsford,
141 U.S. 250 (1891) 16

United States v. Albertini,
472 U.S. 675 (1985) 22

United States v. Apple MacPro Comput.,
851 F.3d 238 (3d Cir. 2017) 43

United States v. Balsys,
524 U.S. 666 (1998) 33, 39

United States v. Burr,
25 F. Cas. 38 (C.C.D. Va. 1807) (No. 14,692e) 40, 41

United States v. Gooseley,
25 F. Cas. 1363 (C.C.D. Va. 1800) (No. 15,230) 40

United States v. Helmsley,
941 F.2d 71 (2d Cir. 1991) 37, 38, 39

United States v. Hubbell,
530 U.S. 27 (2000) 47, 50, 52

United States v. North,
920 F.2d 940 (D.C. Cir. 1990) 38

United States v. Osinger,
753 F.3d 939 (9th Cir. 2014) 15

United States v. Petrovic,
701 F.3d 849 (8th Cir. 2012) 15

United States v. Stevens,
559 U.S. 460 (2010) 13, 31

United States v. Wade,
388 U.S. 218 (1967) 45, 46

United States v. Williams,
553 U.S. 285 (2008) 29, 32

Utah v. Strieff,
136 S. Ct. 2056 (2016) 38

Virginia v. Black,
538 U.S. 343 (2003) 10

Ward v. Rock Against Racism,
491 U.S. 781 (1989) 22, 29

Williams-Yulee v. Fla. Bar,
575 U.S. 433 (2015) 13, 25

Woolsey v. Judd,
11 How. Pr. 49 (N.Y. Sup. Ct. 1855) 14

Yee v. Escondido,
503 U.S. 519 (1992) 51

Statutes

42 U.S.C. § 1320d-6 21

42 U.S.C. § 408 21

Ames Crim. Stat. 545 ..... *passim*

Vt. Stat. Ann. tit. 13, § 2606 (2020) 24

Other Authorities

Charles Fried, *An Anatomy of Values* (1970) 24

Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 Wake Forest L. Rev. 345 (2014) 12, 28, 29

Derek E. Bambauer, *Exposed*,
98 Minn. L. Rev. 2025 (2014) 12

Eugene Volokh, *The Freedom of Speech and Bad Purposes*,
63 UCLA L. Rev. 1366 (2016) 27

New Report Shows that 4% of U.S. Internet Users Have Been a Victim of "Revenge Porn," Ctr. for Innovative Pub. Health Rsch. (Dec. 13, 2016), https://innovativepublichealth.org/press-releases/revenge-porn-report-findings 2

Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L.J. 989 (2018) 33

Orin S. Kerr, *Decryption Originalism: The Lessons of* Burr, 134 Harv. L. Rev. 905 (2021) 40, 41

Revenge Porn Statistics, Cyber C.R. Initiative, https://www.cybercivilrights.org/wp-content/uploads/2014/12/RPStatistics.pdf 3, 23

Richard A. Nagareda, *Compulsion "To Be a Witness" and the Resurrection of* Boyd, 74 N.Y.U. L. Rev. 1575 (1999) 54

Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890) 14

Survivors of Human Trafficking Fight Back Act of 2020, S. 4983, 116th Cong. (2020) 29

Rules

Sup. Ct. R. 14 51

Treatises

1 Leonard MacNally, *The Rules of Evidence on Pleas of the Crown* (London, J. Butterworth & Dublin, J. Cooke 1802) 40

2 Joseph Story, *Commentaries on Equity Jurisprudence* (Boston, Hilliard, Gray & Co. 1836) 14

Restatement (Second) of Torts (Am. L. Inst. 1977) 15

Constitutional Provisions

U.S. Const. amend. I 10

U.S. Const. amend. V 33

OPINIONS BELOW

The Ames Supreme Court's decision affirming Petitioner Laura Tanner's conviction is reproduced at page 2 of the Joint Appendix. The Ames Superior Court's decision denying Petitioner's motion to dismiss is reproduced at page 24 of the Joint Appendix. The Ames Superior Court's decision granting the State's motion to compel is reproduced at page 26 of the Joint Appendix.

JURISDICTIONAL STATEMENT

The Ames Supreme Court affirmed Petitioner's conviction on August 28, 2020. J.A. 16. Her petition for writ of certiorari was granted on January 5, 2021. J.A. 1. This Court has jurisdiction under 28 U.S.C. § 1257(a).

RELEVANT PROVISIONS

This case involves the First and Fifth Amendments to the United States Constitution and the Ames Nonconsensual Pornography Act, Ames Crim. Stat. 545. All relevant provisions are reproduced in the Appendix.

STATEMENT OF THE CASE

This case goes to the heart of "the balance which our Nation, built upon postulates of respect for the liberty of the individual, has struck between that liberty and the demands of organized society." *Poe v. Ullman*, 367 U.S. 497, 542 (1961) (Harlan, J., dissenting). New technologies occasionally require the Court to revisit this balance in a changing world. But "[t]he choice is not between order and liberty." *Terminiello v. City of Chicago*, 337 U.S. 1, 37 (1949) (Jackson, J., dissenting). In this case, Petitioner's challenge to the State's authority to regulate and investigate criminal conduct poses a choice "between liberty with order and anarchy without either." *Id.*

Nonconsensual Pornography

Nonconsensual pornography—the unauthorized distribution of private, intimate images—is an especially damaging problem. More than ten million Americans have had sexually explicit images of themselves distributed or threatened to be distributed online. *New Report Shows that 4% of U.S. Internet Users Have Been a Victim of "Revenge Porn,"* Ctr. for Innovative Pub. Health Rsch. (Dec. 13, 2016), https://innovativepublichealth.org/press-releases/revenge-porn-report-findings. Over ninety percent of victims report significant emotional distress, and forty-two percent seek professional help for mental health problems. *Revenge Porn Statistics*, Cyber C.R. Initiative, https://www.cybercivilrights.org/wp-content/uploads/2014/

12/RPStatistics.pdf. Almost forty percent of victims suffer professional consequences; many lose their jobs and struggle to find new work. *Id.* Nearly half of victims are subsequently harassed and stalked. *Id.* Women, who comprise approximately ninety percent of victims, bear the disproportionate brunt of all these harms. *Id.*

Ames's Response

Recognizing the need for intervention, forty-six states, the District of Columbia, and Guam have passed laws making nonconsensual pornography a crime. J.A. 3. The Ames legislature likewise concluded that nonconsensual pornography is "a major social problem requiring immediate legislative response," Ames Crim. Stat. 545(a)(1), and passed the Nonconsensual Pornography Act (NCPA) in 2016, J.A. 2.

The NCPA combats nonconsensual pornography by making it a crime to disclose sexual images of another person without their consent. Ames Crim. Stat. 545(a)(5), (c). Liability attaches only when (1) the person depicted in the image is identifiable; (2) the distributor of the image knows or should know the person expected the image to remain private; (3) that expectation of privacy is reasonable; and (4) the distributor knows or should know the person depicted did not consent to the disclosure of the image. *Id.* 545(c).

The statute also contains two exceptions. First, it permits disclosures of images "involving voluntary exposure in public or

commercial settings." *Id.* 545(d)(1). Second, it allows disclosures "to a small audience to advance the public interest, including but not limited to the reporting of unlawful conduct to competent authorities." *Id.* 545(d)(2).

This Prosecution

On October 10, 2018, a man with the initials M.S. attempted to send his girlfriend, Laura Taylor, an intimate, sexually explicit video of himself. J.A. 4, 23. Instead, M.S. accidentally sent the video to Petitioner Laura Tanner, J.A. 4, a coworker at Ames Robotics with whom he had rarely interacted, J.A. 22. Petitioner immediately posted the video on a publicly accessible online message board used by Ames Robotics employees. J.A. 4. Before posting on the message board, users see a pop-up warning them not to post "information that should be kept secret" because the website is "not private or secure." J.A. 19. Petitioner's post included the unredacted, ninety-second-long video of M.S. and identified him by name and professional title. J.A. 17, 19.

After M.S. realized his mistake the next day, he apologized to both Petitioner and his colleagues. J.A. 4. He requested that the video be removed from the message board, J.A. 23, and it was taken down that afternoon, J.A. 20. By then, however, the video had already been reposted to at least two pornography websites. J.A. 20. It will likely remain on the internet forever. J.A. 5.

M.S.'s "life and career have been ruined" by nonconsensual pornography. J.A. 5. Soon after the disclosure, he was fired, and he has not been able to find work since. J.A. 5. M.S. has been subject to online harassment and threats, and he sees a psychologist to manage trauma from these events. J.A. 20.

The Ames police investigated Petitioner's conduct as a potential violation of the NCPA. J.A. 5. In an interview, Petitioner stated that she "felt bad about everything that had happened to [M.S.]." J.A. 21. Pursuant to a warrant, police attempted to search Petitioner's computer and cell phone but could not access the information on the devices, as they were password-protected. J.A. 6. Petitioner refused to disclose the passwords, citing the Fifth Amendment privilege against self-incrimination. J.A. 6.

The State filed a criminal complaint against Petitioner for violating the NCPA. J.A. 6. Petitioner moved to dismiss the complaint, challenging the constitutionality of the statute. J.A. 6. The trial court denied the motion, finding that the statute "carves out situations in which the disclosure of [nonconsensual pornography] might actually have social value, leaving behind only valueless disclosures." J.A. 25. As a result, it concluded that the NCPA does not prohibit any speech that is protected by the First Amendment. J.A. 25.

The State then moved to compel Petitioner to disclose the passwords. J.A. 6. The trial court granted the motion, concluding that disclosure of the passwords was "not testimonial in nature under the foregone conclusion exception." J.A. 27. Petitioner entered a conditional guilty plea, reserving her right to appeal, and the trial court accepted the plea. J.A. 28–29. Petitioner then appealed both the denial of the motion to dismiss and the grant of the motion to compel. J.A. 6.

The Ames Supreme Court affirmed both rulings. J.A. 6. First, the court acknowledged "persuasive arguments" that the First Amendment does not protect nonconsensual pornography at all. J.A. 8–9. But the court concluded that, even if the First Amendment applied, the NCPA was constitutional. J.A. 10. Assuming without deciding that strict scrutiny applied, the court held that the statute was narrowly tailored to serve the State's compelling interest in shielding citizens from disclosures because it applied to only a "discrete subset" of speech, J.A. 10, while "preserv[ing] Tanner's right to call out suspected sexual harassment without disclosing the damaging video," J.A. 13. Second, the court concluded that the Fifth Amendment did not prohibit compelled disclosure of the passwords because "the password itself is not testimonial or incriminating." J.A. 16.

This Court granted certiorari. J.A. 1.

SUMMARY OF THE ARGUMENT

I. The court below correctly concluded that the NCPA does not violate the First Amendment. The Ames legislature recognized the rapidly growing problem of nonconsensual pornography and took corrective action. The resulting statute addresses the damage of nonconsensual pornography without inhibiting public discussion.

A. Nonconsensual pornography is not protected by the First Amendment. This Court has recognized that states may criminalize speech within narrow, historically defined categories, including obscenity. Nonconsensual pornography is obscene because it appeals to a prurient interest in others' sexual humiliation, is patently offensive, and has no redeeming value. Alternatively, nonconsensual pornography warrants its own categorical exception based on historical regulation of similar speech and core First Amendment values.

B. Even assuming nonconsensual pornography is protected speech, the NCPA should be subject to only intermediate scrutiny, which it passes. While the statute targets sexual images, criminality turns on the nonconsensual manner of distribution. This Court has applied intermediate scrutiny to other regulations on expression even where they made some reference to content.

C. The NCPA also withstands strict scrutiny. The statute is narrowly tailored to further the State's compelling interests in safeguarding citizens' welfare and privacy. Several provisions curb the

reach of the statute, including a limited subset of covered images, an objective privacy standard, a three-part scienter requirement, and an exception for disclosures in the public interest. No less restrictive alternative exists.

D. The NCPA is not overbroad. The statute prohibits only unprotected speech and would not prevent Petitioner's hypothetical disclosures. Even if the statute does reach some protected speech, any overbreadth is insubstantial.

E. This Court should sever any portions of the statute it deems invalid. Facial invalidation would contravene the legislature's intent and leave victims across Ames defenseless against nonconsensual pornography.

II. Petitioner cannot invoke the Fifth Amendment privilege against compelled self-incrimination to avoid disclosing the passwords to her devices. The Fifth Amendment protects only communications that are both incriminating and testimonial. The passwords meet neither requirement. Moreover, the passwords themselves and the incidental communications that attend their disclosure are foregone conclusions, because they add little or nothing to the government's knowledge. Finally, Petitioner's argument that the Fifth Amendment bars compelled production of private documents falls outside the scope of the question presented and does not resolve the case in her favor.

A. The passwords are not incriminating. They are neither evidence of Petitioner's crimes nor do they lead the State to evidence of the crimes. Although the passwords unlock the devices, they do not form a link in the chain of evidence because their connection with the information on the devices is attenuated. If the State accesses the files on Petitioner's devices, it is because the State bore its evidentiary burden to procure a valid warrant, not because Petitioner revealed the passwords. The original understanding of the Fifth Amendment supports that conclusion. Petitioner's attempt to frame the password disclosure as incriminating would disturb the equilibrium that the Constitution achieves between individual liberty and law enforcement.

B. The passwords are also insufficiently testimonial to receive Fifth Amendment protection. Numerous kinds of disclosures have some testimonial qualities but fall below the necessary threshold to trigger the Fifth Amendment. For example, a suspect's implicit affirmation that a handwriting exemplar is his own writing is not deemed testimonial because it is incidental to the creation of the exemplar. Similarly, the disclosure of the passwords is incidental to Petitioner's authorization of the State to search her phone. The valid purpose predominates over the incidental communication.

C. Further, because the passwords and the incidental disclosures that attend their revelation have minimal significance to the State, they

are foregone conclusions that do not receive Fifth Amendment protection.

D. The question before the Court is whether Petitioner can be compelled to disclose her passwords, not whether she can be compelled to produce private documents. Petitioner's argument that the privilege categorically bars compelled production of private documents is thus not included in the question presented. Regardless, Petitioner's rule confirms the State's authority to compel password disclosure. The State has a warrant to search Petitioner's devices, and the Constitution does not provide Petitioner with relief from an exercise of legitimate police authority.

ARGUMENT

I. The NCPA does not violate the First Amendment.

The protections of the First Amendment "are not absolute." *Virginia v. Black*, 538 U.S. 343, 348 (2003); *see* U.S. Const. amend. I. Nonconsensual pornography is "no essential part of any exposition of ideas" and is of such "slight social value as a step to truth" that it does not receive First Amendment protection. *Chaplinsky v. New Hampshire*, 315 U.S. 568, 572 (1942). But even if nonconsensual pornography is protected, the NCPA survives any level of scrutiny. The statute is narrowly tailored to prevent the nonconsensual distribution of sexual material—a "staggering" problem that has affected millions of Americans, *People v. Austin*, 155 N.E.3d 439, 452 (Ill. 2019), *cert. denied*,

141 S. Ct. 233 (2020) (mem.). Every state supreme court to have considered the issue has concluded that laws like the NCPA are constitutional.

A. The First Amendment does not protect nonconsensual pornography.

The First Amendment does not protect the nonconsensual disclosures of private sexual material that the NCPA prohibits. Nonconsensual pornography fits within the existing categorical exception for obscenity. But even if it does not, nonconsensual pornography warrants an exception in its own right. History and tradition demonstrate that similar speech has never received First Amendment protection.

1. Nonconsensual pornography is obscene.

This Court has "categorically settled . . . that obscene material is unprotected by the First Amendment." *Miller v. California*, 413 U.S. 15, 23 (1973). Material is obscene when it (1) "appeals to the prurient interest" based on contemporary community standards; (2) "depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law"; and (3) "lacks serious literary, artistic, political, or scientific value." *Id.* at 24. The nonconsensual pornography covered by the NCPA satisfies each prong.

First, the NCPA regulates only those images that appeal to the prurient interest. Material appeals to the prurient interest "if it is in

some sense erotic," *Ashcroft v. ACLU*, 535 U.S. 564, 579 (2002), taking into account the manner of creating and disseminating the material, *Splawn v. California*, 431 U.S. 595, 598 (1977). For viewers, these images gratify a desire to see victims humiliated by the exposure of their sexual conduct. *See* Derek E. Bambauer, *Exposed*, 98 Minn. L. Rev. 2025, 2044 (2014). Petitioner is therefore wrong to compare nonconsensual pornography to pornography generally. Pet'r's Br. 15. Compared with the nudity available on thousands of other sites, nonconsensual pornography is unique because it stimulates a perverse thrill in degrading victims through coerced sexual exposure.

Second, the NCPA regulates images that are patently offensive. Even if images of nudity and sexual acts might not be offensive when viewed in isolation, "the setting in which the publications were presented" renders them offensive. *Ginzburg v. United States*, 383 U.S. 463, 465 (1966). Images that "debase[] and distort[]" intimate relationships are frequently deemed offensive. *Paris Adult Theatre I v. Slaton*, 413 U.S. 49, 63 (1973). Nonconsensual pornography does precisely that, as evidenced by victims' humiliation and social isolation. *See* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 Wake Forest L. Rev. 345, 351–54 (2014).

Third, nonconsensual pornography has no cognizable value under *Miller*. There are few circumstances in which nonconsensual disclosures

of sexual images hold any value at all. In those rare cases where distribution *would* serve the public interest, the NCPA includes an exception permitting such disclosures. Ames Crim. Stat. 545(d)(2). Petitioner claims that the statute would prohibit reporting on the Abu Ghraib photos, Pet'r's Br. 30, or the Anthony Weiner scandal, Pet'r's Br. 28. But in both cases, the media redacted the images such that they did not expose an "identifiable person" or "intimate parts." Ames Crim. Stat. 545(c). The NCPA thus permits disclosure of images that would have serious value under *Miller*.

2. Nonconsensual pornography should be identified as a new categorical exception to First Amendment protection.

Even if nonconsensual pornography is not obscene, this Court should recognize it as a new categorical exception. The Court has observed that there may be some categories of historically unprotected speech that "have not yet been specifically identified." *United States v. Stevens*, 559 U.S. 460, 472 (2010). When identifying such categories, a "history and tradition of regulation are important factors." *Williams-Yulee v. Fla. Bar*, 575 U.S. 433, 446 (2015). Here, history and tradition support a new exception for nonconsensual pornography.

a. History supports a categorical exception for nonconsensual pornography.

Historical practice demonstrates that the First Amendment does not protect nonconsensual pornography. The state's ability to enforce

citizens' privacy rights consistent with the First Amendment "has a well-established history in U.S. law." *State v. VanBuren*, 214 A.3d 791, 805 (Vt. 2019); *accord Austin*, 155 N.E.3d at 455. As early as 1841, Justice Story recognized individuals' rights in their "familiar letters" and that courts could "prevent [their] publication by an injunction, as a breach of private confidence." *Folsom v. Marsh*, 9 F. Cas. 342, 346 (C.C.D. Mass. 1841) (No. 4,901). Similarly, other mid-nineteenth-century American courts upheld individuals' right to prohibit disclosures of private letters they had written that others sought to distribute. *See, e.g.*, *Woolsey v. Judd*, 11 How. Pr. 49, 61 (N.Y. Sup. Ct. 1855) (citing *Gee v. Pritchard* (1818) 36 Eng. Rep. 670, 675–76).

Assessing this tradition in a seminal 1890 article titled *The Right to Privacy*, Samuel Warren and Louis Brandeis observed that the "common law secures to each individual . . . the power to fix the limits of the publicity which shall be given his [thoughts, sentiments, and emotions]." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 198 (1890). Privacy rights bolstered free speech because they encouraged free and open communication between private parties without fear of publication. *See* 2 Joseph Story, *Commentaries on Equity Jurisprudence* § 946 (Boston, Hilliard, Gray & Co. 1836).

Petitioner neglects this history and its manifestations in modern First Amendment law. Courts frequently prioritize individuals' right to control their sexual images over the First Amendment rights of other speakers. *See, e.g.*, *United States v. Osinger*, 753 F.3d 939, 948 (9th Cir. 2014) (holding that sexually explicit publications of private individual were not protected); *United States v. Petrovic*, 701 F.3d 849, 855–56 (8th Cir. 2012) (holding that disclosure of "intensely private information" that was "never in the public domain" was not protected). Similarly, states have recognized a cause of action in tort for "publicity given to private life." Restatement (Second) of Torts § 652D (Am. L. Inst. 1977); *see also VanBuren*, 214 A.3d at 806. Today, as in 1841, the law guards the privacy of intimate communications.[1]

b. First Amendment values support a categorical exception for nonconsensual pornography.

Nonconsensual pornography does not advance First Amendment values. "[T]o equate the free and robust exchange of ideas and political debate" with the exploitation of sexual materials "demeans the grand conception of the First Amendment and its high purposes in the historic struggle for freedom." *Miller*, 413 U.S. at 34. The private sexual images

[1] Petitioner discounts this history because statutes like Ames's are a relatively recent phenomenon. Pet'r's Br. 14. But that is because virtual nonconsensual pornography has proliferated with the rise of the internet. Petitioner's argument says nothing about the historical treatment of analogous private communications.

at issue add little to public dialogue. But their nonconsensual distribution undermines sexual privacy interests that this Court has long safeguarded. *See, e.g.*, *Union Pac. Ry. Co. v. Botsford*, 141 U.S. 250, 252 (1891) ("To compel any one . . . to lay bare the body . . . is an indignity, an assault, and a trespass . . . .").

Petitioner disagrees and argues that nonconsensual pornography helps combat sexual harassment. *See, e.g.*, Pet'r's Br. 12, 22, 23, 25, 28. But Petitioner conflates disseminating sexually explicit images with "reporting sexual harassment." Pet'r's Br. 12. Under the NCPA, Petitioner was fully entitled to report that she believed M.S. had harassed her. Nothing in the statute would have stopped her from sharing the video with the police, her supervisor, or human resources. Ames Crim. Stat. 545(d)(2). Petitioner further contends that, in some cases, victims of harassment must use nonconsensual pornography to "broadcast their stories." Pet'r's Br. 22. But they can still do so because the statute allows disclosures of redacted images. And Ames citizens remain free to express their views on workplace harassment. The NCPA thus permits speech on public issues while curtailing the disclosure of images at the heart of individual privacy.

Even if nonconsensual pornography has some value, that does not preclude creating a categorical exception. Child pornography, for example, is unprotected not because it is always without value but

because of how it is produced. *See Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 251 (2002) (recognizing some works of child pornography "might have significant value"). The question, therefore, is how to properly accommodate Petitioner's right to speak, M.S.'s right to privacy, and the public interest. M.S. may be subject to harassment and threats for the rest of his life because the video "is unlikely ever to vanish completely." J.A. 5. To be sure, Petitioner also has an interest in reporting possible harassment, but the NCPA leaves open lawful avenues to do so. Even when those avenues are imperfect, "our law frowns on vigilante justice," *Perma Life Mufflers, Inc. v. Int'l Parts Corp.*, 392 U.S. 134, 154 (1968) (Harlan, J., concurring in part and dissenting in part), and the First Amendment does not "require[] the legislature to condone it," J.A. 13.

As a matter of history and tradition, the First Amendment provides no shelter to damaging distributions of intimate communications. A categorical exception is appropriate because "the evil to be restricted so overwhelmingly outweighs the expressive interests . . . at stake." *New York v. Ferber*, 458 U.S. 747, 763–64 (1982).

B. The NCPA withstands intermediate scrutiny.

Even if the NCPA regulates protected speech, it should be subject to only intermediate scrutiny, which it withstands. Although content-based regulations on speech must survive strict scrutiny, "[d]eciding whether a particular regulation is content based or content neutral is

not always a simple task." *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 642 (1994). Strict scrutiny is appropriate when content discrimination "raises the specter that the Government may effectively drive certain ideas or viewpoints from the marketplace." *Davenport v. Wash. Educ. Ass'n*, 551 U.S. 177, 188 (2007) (quoting *R.A.V. v. City of St. Paul*, 505 U.S. 377, 387 (1992)). In many cases, however, "that risk is inconsequential," and therefore "strict scrutiny is unwarranted." *Id.*

Petitioner oversimplifies the inquiry in this case by insisting that the NCPA is "obvious[ly] content-based." Pet'r's Br. 16 (alteration in original) (quoting *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015)). But like other laws this Court has subjected to intermediate scrutiny, the NCPA "does not . . . fit neatly into either the 'content-based' or the 'content-neutral' category." *City of Renton v. Playtime Theatres, Inc.*, 475 U.S. 41, 47 (1986). It is true that the law refers to images that include "intimate parts" or "sexual act[s]," Ames Crim. Stat. 545(c), but the nonconsensual *manner* of distribution is "crucial to . . . illegality," *Austin*, 155 N.E.3d at 457 (upholding similar law under intermediate scrutiny). Sexually explicit images can still be freely disseminated under the NCPA, so long as the subject has consented or did not have a reasonable expectation that the images would remain private.[2]

[2] Petitioner incorrectly asserts that the NCPA prohibits disclosures "without the express consent of the subject." Pet'r's Br. 2. But if the

On multiple occasions, this Court has applied intermediate scrutiny to laws that made at least some reference to content. In *Members of the City Council v. Taxpayers for Vincent*, 466 U.S. 789 (1984), the Court did not apply strict scrutiny to a sign ordinance that exempted plaques commemorating "historical, cultural, or artistic event[s]." *Id.* at 791 n.1, 804–10. The same was true in *City of Renton*, where the Court applied intermediate scrutiny even though the ordinance at issue "treat[ed] theaters that specialize[d] in adult films differently from other kinds of theaters." 475 U.S. at 47. Here, as in those cases, "there is no realistic possibility that official suppression of ideas is afoot." *Davenport*, 551 U.S. at 189 (quoting *R.A.V.*, 505 U.S. at 390). Petitioner cannot point to a single idea that the NCPA prevents her from expressing. Accordingly, "strict scrutiny is unwarranted." *Id.* at 188.

Reed v. Town of Gilbert, 576 U.S. 155 (2015), does not compel a different conclusion. For one, the *Reed* Court said nothing to indicate it was overruling any of the aforementioned cases. On the contrary, the Court cited *Taxpayers for Vincent* to *support* the proposition that municipalities "may go a long way toward entirely forbidding the posting of signs, so long as [they] do so in an evenhanded, content-neutral

---

distributor does not know—and should not have known—that the subject "reasonably expected that the image would remain private," then express consent is not required. Ames Crim. Stat. 545(c).

manner." *Reed*, 576 U.S. at 173. Petitioner nevertheless implies that whether some of these decisions "remain[] good law" is uncertain. Pet'r's Br. 17. But "[t]his Court does not normally overturn . . . earlier authority *sub silentio*." *Shalala v. Ill. Council on Long Term Care, Inc.*, 529 U.S. 1, 18 (2000). And in fact, three of the six Justices who joined the majority opinion in *Reed* also observed that restrictions on signs "advertising a one-time event" would not be content based. 576 U.S. at 175 (Alito, J., joined by Kennedy and Sotomayor, JJ., concurring). Consistent with *Taxpayers for Vincent* and *City of Renton*, such restrictions would require at least some reference to the content of the signs to determine whether they advertised a one-time or recurring event. This Court should therefore reject Petitioner's suggestion that *Reed* quietly wiped away decades of precedent.

Furthermore, the regulation that triggered strict scrutiny in *Reed* was far broader than the NCPA and explicitly singled out political and ideological speech for differential treatment. The ordinance exempted twenty-three categories of signs from permit requirements, *id.* at 159 (majority opinion), and it "[did] not pass strict scrutiny, or intermediate scrutiny, or even the laugh test," *id.* at 184 (Kagan, J., concurring in the judgment). The ordinance also treated political signs "less favorably than ideological signs." *Id.* at 160 (majority opinion). By contrast, the NCPA does not target speech on matters of public concern. As this Court

has made clear, "First Amendment protections are often less rigorous" in cases that involve "matters of purely private significance." *Snyder v. Phelps*, 562 U.S. 443, 452 (2011). Regulating private material such as nonconsensual pornography poses "no threat to the free and robust debate of public issues," *id.* at 452 (quoting *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 760 (1985) (plurality opinion)), and thus intermediate scrutiny is appropriate.

Subjecting the NCPA to strict scrutiny would have far-reaching negative effects. Under Petitioner's theory, countless other privacy regulations would have to survive this Court's highest standard of review. Rejecting that approach, the Illinois Supreme Court observed that "[t]he entire field of privacy law is based on the recognition that some types of information are more sensitive than others." *Austin*, 155 N.E.3d at 458. For instance, laws that prohibit the unauthorized release of health information, *e.g.*, 42 U.S.C. § 1320d-6, or Social Security information, *e.g.*, 42 U.S.C. § 408(a)(8), would be considered "content based." *See Austin*, 155 N.E.3d at 458. These laws, like the NCPA, target nonconsensual disclosures—not the underlying content itself. While applying strict scrutiny here would do little to preserve the marketplace of ideas, it would subject commonplace regulations to endless litigation.

Under intermediate scrutiny, regulations need only "promote[] a substantial government interest that would be achieved less effectively absent the regulation." *Ward v. Rock Against Racism*, 491 U.S. 781, 799 (1989) (quoting *United States v. Albertini*, 472 U.S. 675, 689 (1985)). There is no doubt that Ames's interests in citizens' welfare and privacy are "served in a direct and effective way" by restrictions on nonconsensual pornography. *Id.* at 800. The NCPA also "leave[s] open ample alternative channels of communication," *id.* at 802, because sexually explicit images may still be freely disseminated where the subject consents, and victims may still "call out suspected sexual harassment" without distributing such material, J.A. 13. The statute should therefore be upheld.

C. The NCPA withstands strict scrutiny.

Even under strict scrutiny, the NCPA is constitutional. Laws that are subject to strict scrutiny must be "narrowly tailored to serve compelling state interests." *Reed*, 576 U.S. at 163. Nonconsensual pornography threatens the State's compelling interests in citizens' welfare and privacy. The NCPA is narrowly tailored to serve those interests, regulating only those images that are truly private and whose disclosure would threaten subjects' welfare. No alternative would be as effective or more speech protective by comparison.

1. Nonconsensual pornography threatens the State's compelling interests in citizens' welfare and privacy.

It is undeniable that the State's interest in regulating nonconsensual pornography is compelling. *See* Pet'r's Br. 21 (conceding the State's compelling interest). Nonconsensual pornography regularly inflicts "harrowing" injuries and destroys victims' lives. *State v. Casillas*, 952 N.W.2d 629, 643 (Minn. 2020). M.S.'s injuries—mental trauma, job loss, and online harassment, J.A. 20—are characteristic of those sustained by victims of nonconsensual pornography, *see Revenge Porn Statistics*, *supra*. Every court to have reached the issue agrees that protecting these victims is a compelling interest. *E.g.*, *Casillas*, 952 N.W.2d at 642–43; *VanBuren*, 214 A.3d at 808.

In addition to avoiding these injuries, the NCPA advances the State's compelling interest in enforcing victims' privacy rights. The State's interest in the privacy of intimate images accords with the interest in individual privacy underlying much of American law. *See supra* pp. 13–15, 21. With respect to sexual privacy, the government's interest is especially strong. *See, e.g.*, *Lawrence v. Texas*, 539 U.S. 558, 567 (2003); *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965).

Recognition of sexual privacy is necessary to "encourag[e] the uninhibited exchange of ideas and information among private parties." *Bartnicki v. Vopper*, 532 U.S. 514, 532–33 (2001) (quoting Brief for the

United States at 27, *Bartnicki*, 532 U.S. 514 (Nos. 99-1687, 99-1728)); *cf.* Charles Fried, *An Anatomy of Values* 140 (1970) ("[P]rivacy is the necessary atmosphere for [love, trust, and affection], as oxygen is for combustion."). By assuring that private sexual images remain private, the NCPA prevents the chilling of speech whose value depends on its privacy.

2. The NCPA is narrowly tailored to advance the State's compelling interests.

Only truly private images implicate the State's interests, and the NCPA restricts its scope accordingly. The statute is limited by constraints on what images are covered, an objective privacy standard, a three-part scienter requirement, and a broad exception for disclosures in the public interest, which work together to curb its reach.

The statute sets firm limits on which disclosures it regulates. First, the statute covers only images that depict "intimate parts" or a "sexual act." Ames Crim. Stat. 545(c). Like other nonconsensual pornography statutes that have withstood strict scrutiny, the NCPA defines "intimate parts" narrowly. *Compare id.* 545(b)(3) (limiting "intimate parts" to "the naked genitals, pubic area, anus, or female post-pubescent nipple"), *with* Vt. Stat. Ann. tit. 13, § 2606(a)(3) (2020) (same). Second, anonymous images are not regulated; subjects must be "identifiable." Ames Crim. Stat. 545(c). Third, the setting must be private: voluntary nudity and sexual acts in "public or commercial

settings" are not punishable. *Id.* 545(d)(1). Disclosures of images that are missing any of these three components are not covered by the statute.[3]

The NCPA's privacy and scienter requirements further narrow its reach. Privacy is assessed objectively, requiring the State to prove subjects "reasonably expected that the image would remain private." *Id.* 545(c); *see also VanBuren*, 214 A.3d at 823 (construing similar language as imposing an objective standard). The scienter requirements are demanding, meaning that "[i]ndividuals are highly unlikely to accidentally violate this statute while engaging in otherwise permitted speech." *VanBuren*, 214 A.3d at 812. Distributors must (1) "knowingly" disclose the image; (2) "know[] or should know" of subjects' reasonable privacy expectations; and (3) "know[] or should know" that subjects did not consent to disclosure. Ames Crim. Stat. 545(c). This Court requires nothing more and has tolerated much less. Restrictions lacking any sort of scienter element have been upheld under strict scrutiny. *See, e.g.*, *Williams-Yulee*, 575 U.S. at 439. At most, this Court has asked for "*some*

[3] Petitioner argues that the statute is underinclusive because it excludes images of online sex workers in commercial settings. Pet'r's Br. 23. But privacy interests in the workplace are more limited than privacy interests in residential or other personal settings because the subjects are voluntarily exposing themselves to a larger audience for profit. *See O'Connor v. Ortega*, 480 U.S. 709, 725 (1987). In any event, Ames "need not address all aspects of a problem in one fell swoop; policymakers may focus on their most pressing concerns." *Williams-Yulee*, 575 U.S. at 449.

element of scienter." *Ferber*, 458 U.S. at 765 (emphasis added); *see also Hamling v. United States*, 418 U.S. 87, 120–24 (1974) (cataloging cases). The constraints in the NCPA exceed this Court's standards for what strict scrutiny requires.

A broad public interest exception permits disclosures of images that are not purely private. The statute exempts disclosures "to advance the public interest" and provides a capacious list, "including but not limited to" disclosures for such purposes as law enforcement or medical treatment. Ames Crim. Stat. 545(d)(2). The legislature properly limited disclosures to a "small audience" to prevent excessive injury to subjects. *Id.* Since large-scale disclosures threaten grievous harm to subjects' welfare and privacy, the State has a corresponding interest in avoiding unnecessary exposures.

Petitioner raises three objections to the NCPA's tailoring, all of which are misguided. First, Petitioner argues that the "small audience" exception prohibits reporting sexual harassment. Pet'r's Br. 22. As discussed above, the statute does no such thing. *See supra* pp. 16–17. The statute does not interfere with verbal complaints or the distribution of redacted images. The public interest exception also allows criminal reporting and disclosures to "competent authorities." Ames Crim. Stat. 545(d)(2).

Second, contrary to Petitioner's argument, the NCPA permits disclosures of unwelcome photos to friends for private reasons. Pet'r's Br. 21. The NCPA forbids only "transferring, publishing, distributing, or reproducing" such images. Ames Crim. Stat. 545(b)(1). *Showing* a photo to a friend—without sending it—does not fall under any of these categories, and it does not result in the kind of "proliferat[ion] beyond control" that the legislature sought to eradicate. *Id.* 545(a)(5). In any case, the public interest exception exempts showing unwelcome photos to friends. Like disclosures for medical treatment, *id.* 545(d)(2), disclosures that would allow victims to seek emotional support from a friend "advance the public interest" in citizen welfare, and the statute permits them.

Third, the statute need not and should not include an intent-to-harm element. Pet'r's Br. 25. Including a malice requirement would undermine the State's interests because regardless of what the distributor intended, the harm of nonconsensual pornography to victims remains the same. Eugene Volokh, *The Freedom of Speech and Bad Purposes*, 63 UCLA L. Rev. 1366, 1405–06 (2016). Limiting the statute as Petitioner suggests would leave large swaths of victims—including M.S.—without support. That might render the NCPA underinclusive since the statute would fail to reach images that implicate the State's compelling interests.

3. The NCPA is the least restrictive means of advancing the State's interests.

The NCPA is the least restrictive means of advancing Ames's interests. A "less restrictive alternative" must be both more protective of speech and as effective as the regulation being challenged. *Reno v. ACLU*, 521 U.S. 844, 874 (1997). Petitioner's proposed alternatives—civil liability, third-party regulations, and a more precise statute—are inferior or unnecessary.

First, civil liability is not a less restrictive alternative. Criminal liability is the most effective mechanism to "dry up the market" for nonconsensual pornography. *Ferber*, 458 U.S. at 759. Civil liability fails to deter judgment-proof perpetrators and shifts the burden of holding them accountable onto victims, many of whom lack the resources to bring their own suits. *See* Citron & Franks, *supra*, at 358, 361. Forty-six other states have recognized the inadequacy of civil enforcement and deemed criminal liability necessary to restrict the distribution of nonconsensual pornography. *See Austin*, 155 N.E.3d at 453.

A civil remedy would not protect any more speech than the NCPA. Courts have recognized that, for nonconsensual pornography, the "permissible constitutional scope of civil remedies and criminal remedies is the same." *Casillas*, 952 N.W.2d at 644 n.10; *see also VanBuren*, 214 A.3d at 813–14. In fact, civil lawsuits may chill more speech than criminal prosecutions, since criminal prosecutions impose

unique procedural safeguards such as requiring an indictment and proof beyond a reasonable doubt. *N.Y. Times Co. v. Sullivan*, 376 U.S. 254, 277 (1964).

Next, Petitioner suggests regulating third-party employers and internet platforms. Pet'r's Br. 24. These proposals address only a fraction of the harms the NCPA targets. Victims of nonconsensual pornography suffer harms well beyond the workplace. *See supra* pp. 2–3. Platform restrictions do not reach offline distributions, *see* Citron & Franks, *supra*, at 351, and they neglect the many online distributions in which platforms lack knowledge of perpetrators' activities, *see* Survivors of Human Trafficking Fight Back Act of 2020, S. 4983, 116th Cong. § 2 (2020) (requiring knowledge or intent to distribute). In contrast to these piecemeal attempts, the NCPA punishes nonconsensual pornography at its source and thereby prevents the full range of harms stemming from distribution.

Finally, Petitioner argues the statute's public interest exception could be more precise. But "perfect clarity and precise guidance have never been required" of statutory language. *Ward*, 491 U.S. at 794. The NCPA provides sufficient guidance for an ordinary person to determine whether conduct is culpable. *See United States v. Williams*, 553 U.S. 285, 304 (2008).

The statutory examples of law enforcement, legal proceedings, and medical treatment elucidate the meaning of "small audience." Ames Crim. Stat. 545(d)(2). In this context, "small" refers to a setting with a limited number of people that ensures the subject's privacy can be retained. Similarly, "public interest" must be read in light of the statute's other limiting provisions.[4] A reasonable person would understand that reporting criminal conduct, abuse, or harassment falls under the term "public interest" in a statute designed to prevent sexual abuse. At minimum, the ambiguity Petitioner suggests is irrelevant to narrow tailoring because, as explained above, no alternative phrasing would be more protective of speech or as effective at preventing harm compared to the NCPA.[5]

D. The NCPA is not overbroad.

Facial invalidation under the overbreadth doctrine is "strong medicine." *Broadrick v. Oklahoma*, 413 U.S. 601, 613 (1973). A statute

---

[4] Petitioner questions whether the public interest determination is objective or subjective, Pet'r's Br. 25, but the Ames Supreme Court concluded that the disclosure must actually promote the public interest, J.A. 7 (holding disclosure was not in public interest "even if Tanner reasonably believed at the time that it was").

[5] To the extent Petitioner's vagueness argument could be read as an independent facial challenge to the statute, that attempt to invalidate the NCPA must fail. Vagueness is an outgrowth of due process, not the First Amendment, and a speaker "whose speech is clearly proscribed cannot raise a successful vagueness claim." *Holder v. Humanitarian L. Project*, 561 U.S. 1, 20 (2010). A publicly accessible website used by 183 employees is not a small audience, and thus the statute clearly proscribed Petitioner's speech.

is facially unconstitutional only if "a substantial number of its applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep." *Stevens*, 559 U.S. at 473. Because facial invalidation would allow harmful, unprotected speech to go unpunished, the overbreadth doctrine is used "sparingly and only as a last resort." *Broadrick*, 413 U.S. at 613.

Even if the NCPA reaches some protected speech, *but see supra* Section I.A, any overbreadth is not "substantial." As discussed above, the statute is narrowly drawn to cover only "a certain and limited category of knowing conduct." *Austin*, 155 N.E.3d at 468 (rejecting overbreadth challenge to statute with similar limiting features). Instead of considering the overall operation of the statute, Petitioner emphasizes the "bizarre" facts of this case to try to establish overbreadth. Pet'r's Br. 30 (quoting J.A. 12). But these unusual circumstances cannot prove, as Petitioner must, that based on the text of the statute there are a substantial number of unconstitutional applications. *N.Y. State Club Ass'n v. City of New York*, 487 U.S. 1, 14 (1988).

Petitioner attempts to bolster her overbreadth claim with a series of peripheral examples that are not actually regulated by the NCPA. Pet'r's Br. 29–30. The statute does not bar the disclosure of redacted images of sexual harassment or Abu Ghraib prisoners. *See supra* pp. 13, 16. Nor does it prohibit a victim in need of emotional support from

showing an image to a friend. *See supra* p. 27. Petitioner's arguments to the contrary "demonstrate nothing so forcefully as the tendency of [the] overbreadth doctrine to summon forth an endless stream of fanciful hypotheticals." *Williams,* 553 U.S. at 301. Petitioner thus fails to show that overbreadth exists, let alone that it is substantial.

E. This Court should sever any portions of the NCPA that it deems invalid.

It is a "cardinal rule[]" of statutory interpretation that a court should not extend invalidation "further than necessary to dispose of the case before it." *Brockett v. Spokane Arcades, Inc.*, 472 U.S. 491, 501–02 (1985). If at all possible, this Court "prefer[s] . . . to enjoin only the unconstitutional applications of a statute while leaving other applications in force." *Ayotte v. Planned Parenthood of N. New Eng.*, 546 U.S. 320, 328–29 (2006). The "touchstone" for this inquiry "is legislative intent." *Id.* at 330.

Here, the Ames legislature explicitly made the NCPA severable. Ames Crim. Stat. 545(g). If the Court were to find that the "small audience" requirement renders the statute unconstitutional, it should sever that language, thereby permitting any disclosures that are in the public interest. Similarly, if the Court were to find negligence insufficient to impose liability, it should sever the negligence portion of the disjunctive phrase "knows or should know." Ames Crim. Stat. 545(c). Severing objectionable parts of the statute would avoid the "wide-

reaching effects," *Ferber*, 458 U.S. at 769, of complete invalidation and would preserve Ames's ability to support the growing number of people harmed by nonconsensual pornography.

II. Compelled password disclosure does not violate the Fifth Amendment.

"In our judicial system, the public has a right to every man's evidence." *Trump v. Vance*, 140 S. Ct. 2412, 2420 (2020) (internal quotation marks omitted). The Fifth Amendment's guarantee that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself" provides limited relief from this rule. U.S. Const. amend. V. Although the privilege advances liberty interests, it also preserves the Fifth Amendment's "balance of private and governmental interests." *United States v. Balsys*, 524 U.S. 666, 693 (1998).

In this case, Petitioner seeks to upset the Fifth Amendment's balance by expanding the privilege past this Court's precedents and the Constitution's original meaning. By locking a device with a password, criminals can render evidence "beyond the reach of any current or near-future technologies." Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 Geo. L.J. 989, 994 (2018). This Court should affirm that the Fifth Amendment does not privilege the disclosure of the password to a device that the government intends to search pursuant to a warrant.

In order to invoke the privilege, Petitioner must show that communication of her passwords is incriminating, testimonial, and compelled. *Hiibel v. Sixth Jud. Dist. Ct.*, 542 U.S. 177, 189 (2004). Here, the compelled password disclosure is neither incriminating nor testimonial. First, the passwords themselves have no inculpatory value, and the fact that the passwords are causally necessary to execute a lawful search of seized evidence does not establish that the passwords are a link in the chain of evidence. Second, the passwords' testimonial contents fall below the threshold that this Court has recognized as constitutionally significant. Third, the passwords and other information incidental to their disclosure add little or nothing to the government's knowledge, making the passwords' disclosure a foregone conclusion. Finally, Petitioner's attack on the compelled production of private documents is immaterial to this case, and Petitioner's logic would in fact permit the government to compel password disclosure.

A. Compelled password disclosure is not incriminating.

For Petitioner's passwords to be incriminating, they must "furnish a link in the chain of evidence needed to prosecute" her. *Hoffman v. United States*, 341 U.S. 479, 486 (1951); *see also Kastigar v. United States*, 406 U.S. 441, 445 (1972) (holding that disclosures that may "lead to other evidence" cannot be compelled). Petitioner claims that the password disclosure is incriminating because "it would allow

the police to access the cell phone and computer in Tanner's possession." Pet'r's Br. 32. But under this Court's precedents and the Fifth Amendment's original meaning, a string of characters devoid of evidentiary value is not "a link in the chain of evidence."[6] Although a communication need not contain inculpatory evidence to be incriminating, the information sought must at least generate suspicion or leads for further investigation. These passwords do neither; they only let police perform a search. Adopting Petitioner's erroneous theory of purely causal incrimination would dramatically expand the privilege without justification.

1. A password is not incriminating because it is a sequence of characters with no evidentiary value.

A password is merely "a series of characters without independent evidentiary significance." *State v. Andrews*, 234 A.3d 1254, 1275 (N.J. 2020). Those characters are disconnected from facts about the crime. If the State knew Petitioner's passwords, it would not know any more about Petitioner's criminal activities than it knows now. It would know only the sequence of characters that happens to unlock Petitioner's devices, and it could infer nothing about Petitioner or her conduct from

[6] In this section the State addresses the non-incriminating nature of the passwords themselves. Incidental disclosures attending the disclosure of the passwords (for example, that Petitioner knows the passwords) are not protected by the Fifth Amendment either, for reasons explained in Section II.C.

that sequence. The passwords' utility for unlocking the devices does not render them incriminating, even if there is incriminating information located on the devices.[7]

Hoffman v. United States, 341 U.S. 479 (1951), illustrates why a password is not a link in the chain of evidence. Called to testify before a grand jury, Hoffman had refused to answer questions about his contacts with a fugitive witness named Weisberg. *Id.* at 481. The Court held that the privilege protected Hoffman's refusal because his answers "would establish contacts" with Weisberg "during the crucial period when [Weisberg] was eluding the grand jury." *Id.* at 488. Those contacts could have aroused suspicion that Hoffman was engaged in criminal activity. By contrast, Petitioner's passwords would not generate any suspicion about her or her activities.

2. Petitioner's purely causal theory of incrimination is inconsistent with this Court's precedents.

Petitioner assumes, without argument, a purely causal theory of incrimination. Under this theory, that a communication is a but-for

[7] Passwords may theoretically contain incriminating information. For example, Petitioner's password could be "IpostedtheMSvideo." But neither Petitioner nor the record raises this possibility, and passwords ordinarily are not incriminating in this fashion, even if they do incorporate personal information such as birthdates. *See Hiibel*, 542 U.S. at 190–91 (rejecting theory that disclosure of name would be incriminating because the disclosure is "incriminating only in unusual circumstances" and the risk must be "real and appreciable").

cause of the State's eventual access to inculpatory evidence suffices to make that communication incriminating. That sweeping theory of incrimination has no basis in this Court's precedents, the Fifth Amendment's original meaning, or the policies underlying the privilege.

This Court held in *Kastigar v. United States*, 406 U.S. 441 (1972), that disclosures that "lead to" inculpatory evidence are protected by the privilege, *id.* at 445, but *Kastigar* did not alter the standard enunciated in *Hoffman*, *id.* at 445 n.11 (citing *Hoffman*, 341 U.S. at 486). The best reading of *Kastigar* is that there must be a proximate relationship between a witness's communication and the evidence to which it leads the government. *See United States v. Helmsley*, 941 F.2d 71, 81–82 (2d Cir. 1991) (analyzing attenuation of causation while applying *Kastigar*). Where the government's lawful actions, rather than the communication itself, are the proximate cause for the discovery of evidence, the relationship between the witness's communication and the evidence is too attenuated to satisfy *Kastigar*. In this case, the government has already borne its evidentiary burden by procuring a valid warrant to search the devices. There is no danger that the government might manipulate Petitioner's disclosure to discover evidence beyond the scope of that warrant.

As is the case in other areas of criminal procedure, simple but-for causation is not enough to meet the *Kastigar* standard. *Helmsley*, 941

F.2d at 82; *United States v. North*, 920 F.2d 940, 957–58 (D.C. Cir. 1990) (Wald, C.J., dissenting) (discussing how Fifth Amendment requires analysis of causal attenuation); *cf. Utah v. Strieff*, 136 S. Ct. 2056, 2059 (2016) (holding that discovery of arrest warrant for suspect during unlawful stop "attenuated the connection between the unlawful stop and the evidence seized incident to arrest," rendering evidence admissible). If the police were to access files on Petitioner's devices, the proximate cause would be not Petitioner's disclosure of the passwords, but rather the lawfully issued warrant.[8] The disclosure thus cannot be said to lead to the files on the devices.

The Second Circuit's analysis in *Helmsley* illuminates why the simplistic but-for test Petitioner suggests is incorrect. After Helmsley gave immunized testimony before a grand jury, a journalist investigated her and published an article detailing her criminal activity. 941 F.2d at 79. That article and its sources provided the basis for Helmsley's subsequent criminal prosecution. *Id.* at 81. Thus, a but-for causal relationship linked Helmsley's immunized testimony and the prosecution's ability to procure the evidence that supported her conviction. But the Court nevertheless held that the Fifth Amendment was not implicated, as there was no "evidentiary use" of her statements

[8] This is only the case where the disclosure has no purpose except permitting the search. The State still cannot compel the answer to a question like, "Where is the evidence?"

nor any "serious danger of manipulative use of the fact of her testimony." *Id.* at 83. The immunized testimony did not illegitimately reduce the government's evidentiary burden.

Precisely the same can be said of Petitioner's passwords in this case. They have no evidentiary significance, and the State's purpose in compelling her to disclose them—execution of a lawful warrant—is plainly not manipulative. Without cooperation from Petitioner, the State has acquired sufficient evidence to meet the Fourth Amendment probable cause standard and persuaded a disinterested magistrate to issue a warrant. By doing so, the State has met its burden of showing that it has an "independent, legitimate source for the disputed evidence." *Id.* at 81 (quoting *Murphy v. Waterfront Comm'n*, 378 U.S. 52, 79 n.18 (1964), *abrogated on other grounds by United States v. Balsys*, 524 U.S. 666 (1998)). For that reason, the warrant, not disclosure of the passwords, is the proximate cause of the State's ability to access files on the devices. That a password is necessary to access the devices at all is "largely fortuitous," much like the causal chain in *Helmsley*. *Id.* at 82. The Fifth Amendment privilege thus has no application here.

3. Both Petitioner's purely causal theory and her conclusion that password disclosure is incriminating are inconsistent with the original understanding of the privilege.

The Founding generation saw the Fifth Amendment privilege as coextensive with the common law privilege. *See* Orin S. Kerr, *Decryption*

Originalism: The Lessons of Burr, 134 Harv. L. Rev. 905, 951–52 (2021). And the common law did not treat communications that caused the discovery of further evidence as incriminating. *See id.* at 953. Rather, incrimination required that the answer itself provide some amount of evidence. *See id.*

The original privilege did not reach statements that cause additional evidence to surface but have no other tendency to incriminate. *See id.* at 938–40. For example, in *United States v. Gooseley*, 25 F. Cas. 1363, 1364 (C.C.D. Va. 1800) (No. 15,230), Justice Iredell described the privilege as reaching questions "leading to an implication of" the witness. None of the relevant cases or treatises supports a broader framing of the privilege. *See, e.g.*, 1 Leonard MacNally, *The Rules of Evidence on Pleas of the Crown* 256–58 (London, J. Butterworth & Dublin, J. Cooke 1802).

Chief Justice Marshall's decision in *United States v. Burr*, 25 F. Cas. 38 (C.C.D. Va. 1807) (No. 14,692e), illustrates how the original standard should be applied to password disclosure. The case concerned a grand jury investigation of Aaron Burr for treason. Kerr, *supra*, at 916–17. Burr had used ciphers to keep his letters private. *Id.* at 918–19. The prosecution sought testimony from Charles Willie, Burr's secretary. *Id.* at 922–23. When the prosecution asked if he knew the cipher, Willie refused to answer. *Id.* at 923. The question then was whether a witness

who admitted knowledge of a cipher encrypting a treasonous letter incriminated himself in misprision of treason. Chief Justice Marshall ruled Willie could not invoke the privilege. *Burr*, 25 F. Cas. at 40.

Burr tracked the common law. A person may refuse to provide an answer that "may disclose a fact which forms a necessary and essential link in the chain of testimony, which would be sufficient to convict him of any crime." *Id.* Incrimination is about the tendency of an answer to prove a crime, not about whether the answer causes more testimony to come to light. For Chief Justice Marshall, disclosing knowledge of a cipher did not amount to self-incrimination. The disclosure established knowledge only at the time of questioning and did not permit the inference that the witness knew the cipher when the treason was alleged to have occurred. *Id.* Similarly, disclosure of the cipher itself would not tend to prove that the witness knew the contents at the time of the treason.

Just as disclosed knowledge of a cipher or disclosure of the cipher itself are not incriminating under the original understanding, neither is disclosure of a password that decrypts a device. As Professor Orin Kerr argues by analogy to *Burr*, "[i]n both instances, the disclosure does not show the key fact that would lead to incrimination." Kerr, *supra*, at 955. So long as knowledge of the password or the password itself does not tend to prove an element of the crime, then the fact that the password

leads police to discover evidence does not establish incrimination as the Founding generation understood it. In this case, Petitioner's knowledge of the passwords does not tend to prove the NCPA offense. The government has a warrant to search Petitioner's devices, and whatever evidence the disclosure causes the police to discover is already in the government's hands.

4. Even if Petitioner's purely causal theory of incrimination found support in this Court's precedents, it should not apply in this case.

Petitioner's theory of incrimination has no basis in this Court's precedents. But even if this Court had adopted the purely causal theory, technological advancements provide a compelling reason not to extend it to cases like this. As this Court has recognized, new technology sometimes requires adapting existing doctrine to protect the balance between individual liberty and the government's ability to guarantee public safety. *See, e.g.*, *Riley v. California*, 573 U.S. 373, 386 (2014) (declining to extend search-incident-to-arrest exception to cell phone searches); *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (declining to extend the third-party doctrine to cell-site location information). In the Fourth Amendment context, mechanical applications of existing doctrine would insufficiently protect individual liberty. But here, in the Fifth Amendment context, new technology

threatens to provide an impenetrable shield to criminals, leaving the police unable to enforce the law.

Today, nearly everyone owns a device that can be encrypted. This was unimaginable when *Kastigar* was decided in 1972. Though "mechanical application" of some language from *Kastigar* may appear to favor blanket application of a purely causal theory of incrimination, to do so would fail to "strike[] the appropriate balance" in this new context. *Riley*, 573 U.S. at 386. Because passwords have no evidentiary value, Petitioner is not helping the government build its case by giving them up. Petitioner is only being prevented from putting an obstacle in the government's way that would all but obliterate its ability to investigate crime.

The drastic expansion of the privilege requested by Petitioner would destroy the "fair state-individual balance" that this Court's Fifth Amendment jurisprudence has preserved. *Doe v. United States* (*Doe II*), 487 U.S. 201, 212 (1988) (quoting *Murphy*, 378 U.S. at 55). Every computer would effectively become a warrant-proof evidence locker, preventing the police from prosecuting serious cybercrimes. *See, e.g.*, *United States v. Apple MacPro Comput.*, 851 F.3d 238, 247–48 (3d Cir. 2017) (involving child pornography on encrypted hard drives). Given these consequences, this Court should not further depart from the privilege's original meaning. *Cf. United States v. Patane*, 542 U.S. 630,

643 (2004) (declining to extend *Miranda v. Arizona*, 384 U.S. 436 (1966)).

Law enforcement's response to this difficulty would, counterintuitively, pose a greater threat to individual privacy rights than permitting compelled decryption. If the government cannot search devices pursuant to a valid warrant, it will be forced to resort to more coercive and invasive means of recovering digital information. The government could pressure technology companies to force users to keep data in external storage accessible to the company, where the government can conduct routine and programmatic searches of digital information. Those kinds of programmatic searches traditionally require no suspicion whatsoever. *See Brigham City v. Stuart,* 547 U.S. 398, 405 (2006). This Court should not participate in Petitioner's quest to turn the privilege into a weapon to destroy evidence acquired by a lawful search warrant.

B. Compelled password disclosure is insufficiently testimonial to warrant application of the privilege.

The Fifth Amendment protects against only the compulsion of communications that are testimonial. *Doe II,* 487 U.S. at 207. As Petitioner points out, a necessary condition for communications to be testimonial is that they "relate a factual assertion or disclose information." Pet'r's Br. 32 (quoting *Doe II*, 487 U.S. at 210). But as this Court's precedents demonstrate, the line between testimonial and non-

testimonial communications is anything but clear. All kinds of compelled acts necessarily convey information, but they are nevertheless not "deemed to be sufficiently testimonial for purposes of the privilege." *Fisher v. United States*, 425 U.S. 391, 411 (1976).

When the government compels the defendant to take an action that communicates information incidental to the government's purpose in compelling the action, the action is insufficiently testimonial for the privilege to apply. For example, one who furnishes a handwriting exemplar "admits his ability to write and impliedly asserts that the exemplar is his writing." *Id.* But it is obvious that the government, when it compels the creation of a handwriting exemplar, is seeking not these admissions but the exemplar itself. So too here. What the State seeks is authorization to access information on the devices. Disclosure of the passwords is purely incidental to that authorization. The testimonial significance of the contents of the passwords is *de minimis*, such that the purpose of authorizing the State's access to the devices predominates and the Fifth Amendment does not apply.

In a simple case, it might suffice to say that a compulsion order requires a person to "disclose information" and is unlawful on that basis. *See* Pet'r's Br. 33 (quoting *Doe II*, 487 U.S. at 210). But if that were the whole of the inquiry there would be no way to explain this Court's decisions in *United States v. Wade*, 388 U.S. 218 (1967), *Gilbert v.*

California, 388 U.S. 263 (1967), and *Fisher*. In each of these cases, the Court permitted the government to compel persons to engage in acts that necessarily conveyed information. One who furnishes a voice exemplar, *Wade*, 388 U.S. at 222, or handwriting exemplar, *Gilbert*, 388 U.S. at 266, implicitly affirms that the exemplar is an accurate representation of his voice or handwriting. Likewise, one who furnishes papers in response to a subpoena for specified documents "tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer." *Fisher*, 425 U.S. at 410. In each of these cases, however, the testimonial significance of the compelled acts was incidental to achieving some other valid purpose, such that the acts were not "deemed to be sufficiently testimonial for purposes of the privilege." *Id.* at 411. The incidental testimony that necessarily accompanies the production of some evidence does not always confer the protection of the Fifth Amendment for that evidence.[9]

This case is analogous to *Doe II* insofar as the State seeks authorization to access the files on Petitioner's devices. In that case, this

[9] The State's argument is not that the insignificance of the testimonial aspect of a communication alone renders it unprotected by the Fifth Amendment. Even insignificant testimonial communications are sufficiently testimonial when they are not incidental to some other valid purpose. *See Pennsylvania v. Muniz*, 496 U.S. 582, 598 (1990) (holding that answering "I don't know" when asked the date of one's sixth birthday is testimonial). But here, unlike in *Muniz*, the disclosure of the password is purely incidental to authorizing the State to do what it has the right to do—search the devices.

Court held that a person could be compelled to execute a consent directive authorizing his bank to disclose information regarding any accounts he might have. 487 U.S. at 218. The Court found it significant that the consent directive "does not point the Government toward hidden accounts or otherwise provide information that will assist the prosecution in uncovering evidence." *Id.* at 215. The same can be said of the passwords in this case. They function as instructions to a device to permit the State to examine its contents, and they tell the State nothing about where evidence might be found. Of course, the passwords are composed of information, such that authorizing a device to yield its contents to the State necessarily involves the disclosure of information, but that disclosure is purely incidental to the authorization. Because the State has no real interest in the passwords themselves, this Court should deem them to be insufficiently testimonial to trigger the privilege.

This Court's dicta indicating that disclosing the combination to a wall safe is testimonial do not change the analysis. *United States v. Hubbell*, 530 U.S. 27, 43 (2000); *Doe II*, 487 U.S. at 219 (Stevens, J., dissenting). First, this Court has not squarely held in any case that the revelation of the combination to a safe is testimonial. That question has not been briefed and subjected to adversarial testing, so it would be improper to conclude that this Court's pronouncements on the matter

are binding. *See Cent. Va. Cmty. Coll. v. Katz*, 546 U.S. 356, 363 (2006). Second, the password for an electronic device is different from the combination to a safe. Because it is generally practicable to open a safe using force, shielding a safe's combination from compelled disclosure does not present a potentially insurmountable obstacle to law enforcement in the way that shielding disclosure of device passwords does. Protecting safe combinations would not dramatically shift the balance of power between law enforcement and criminals. That basic fact about policing at least partially explains why this Court was willing to address the issue in dicta. Since the stakes in this case and cases like it are much higher, it would be inappropriate to uncritically treat them as analogous to hypothetical safe combination cases.

C. Compelled password disclosure is permitted under the foregone conclusion exception because the disclosure would not meaningfully add to the State's knowledge.

The foregone conclusion exception holds that the government may require a defendant to produce testimonial and incriminating evidence when that production "adds little or nothing to the sum total of the Government's information." *Fisher*, 425 U.S. at 411. Here, the government already knows all the information that the password disclosure implicitly asserts.

The foregone conclusion analysis concerns what the act of disclosing the passwords implicitly reveals. In *Fisher*, the Court

explained that an implicit assertion that is "a near truism" or "self-evident" falls outside the privilege. *Id.* After all, those assertions are not at stake in the government's case. Courts applying the exception to password disclosure have correctly recognized three implicit assertions: (1) that the devices are password-protected; (2) that the defendant is aware of the password and can unlock the devices; and (3) that the password is authentic. *See Andrews,* 234 A.3d at 1274–75 (adopting similar test).

Here, all three of those assertions are near-truisms or self-evident. The first assertion is undisputed. *See* J.A. 6, 26. The record does not reflect any controversy over the second, despite Petitioner's belated, implausible attempt to suggest she is unaware of the passwords to her own devices. *Compare* Pet'r's Br. 48–49 (suggesting Petitioner's knowledge of the passwords has not been established), *with* J.A. 26 ("[T]he only person who knows the password is the defendant."). And the passwords authenticate themselves when they unlock the devices. *See, e.g.*, *State v. Stahl*, 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016). Thus, the government can establish all three implicit assertions that turning over the passwords would reveal and "no constitutional rights are touched" by compelling disclosure. *In re Harris*, 221 U.S. 274, 279 (1911).

Petitioner makes two fatal errors of analysis in applying the foregone conclusion exception. First, this Court has never communicated that *Fisher* is bound to its facts such that its reasoning extends only to business records or documents. To the contrary, *Fisher* "applied basic Fifth Amendment principles" and "did not purport to establish a . . . narrow boundary applicable to acts alone." *Doe II*, 487 U.S. at 209. While it is true that *Fisher* involved document subpoenas, the foregone conclusion exception is not limited to that factual context.

Second, Petitioner distorts the foregone conclusion analysis in asserting that the government must already know the contents of either the passwords or the devices. The doctrine focuses on implicit assertions made by password disclosures, not on the contents of the passwords or the devices. For this reason, *Fisher* analyzed whether the act of producing subpoenaed documents would reveal the "existence and possession" of documents beyond what the government knew. *See* 425 U.S. at 411–13. The Court did not consider the substantive contents of the subpoenaed documents because analysis of the relevant implicit assertions was "a question that is distinct" from analysis of the documents themselves. *Hubbell*, 530 U.S. at 37. It is the government's knowledge about the implicit assertions that controls application of the exception.

D. Petitioner's argument that the Fifth Amendment categorically bars compelled production of private documents is immaterial to this case.

This Court should not extend the privilege to shield private documents from subpoenas and Petitioner's arguments to the contrary are outside the scope of the question presented. There is no subpoena for documents here, and producing subpoenaed documents is not analogous to disclosing passwords. Petitioner asks this Court to fashion a constitutional rule without foundation in the record. But even if the argument were properly before the Court, Petitioner's rule would not decide this case. The common law supports the government's authority to compel password disclosure, and in any event the contents of a device fall outside the class of private documents that Petitioner identifies as privileged.

1. Petitioner's argument is outside the scope of the question presented.

The rules of this Court require that "[o]nly the questions set forth in the petition or fairly included therein, will be considered." Sup. Ct. R. 14.1(a). Even "related" or "complementary" questions are not "fairly included." *Yee v. Escondido*, 503 U.S. 519, 537 (1992). "Only in the most exceptional cases" should this Court disregard Rule 14.1(a)—for example, where a constitutional question may be resolved on nonconstitutional grounds. *Izumi Seimitsu Kogyo Kabushiki Kaisha v.*

U.S. Philips Corp., 510 U.S. 27, 32–33 (1993) (internal citations omitted).

This Court granted certiorari to resolve the question "[w]hether the Fifth Amendment privilege . . . allows a defendant to refuse to disclose the password to her computer and phone, when the government has a warrant to search those devices." J.A. 1. Neither that question nor the facts of this case concern subpoenas for private documents.

To make her argument seem relevant to the question presented, Petitioner incorrectly equates password disclosure to "[producing] . . . private documents."[10] Pet'r's Br. 31. But document production means locating and surrendering documents in compliance with a subpoena. *See Hubbell*, 530 U.S. at 43. The government, not Petitioner, will be locating the documents in this case. *Doe II* illustrates the point. There, the government sought to force Doe to sign a form that consented to bank record disclosures. 487 U.S. at 203. The Court did not analogize the signature to document production. *See id.* at 210. After all, the bank would produce the records, not Doe. *Id.* at 216. Like the bank in *Doe II*, here, it is the State that produces the device contents. *See Andrews*, 234

[10] Petitioner limits her theory to private documents to avoid undermining *Fisher*. *See* Pet'r's Br. 37, 41–42. But Justices Thomas and Gorsuch, in their developments of the same theory, reached the opposite conclusion: the government cannot compel the production of any evidence, business records included. *See* Pet'r's Br. 38.

A.3d at 1273 (holding "foregone conclusion test applies to the production of the passwords themselves, rather than to the phones' contents").[11] Ames did not file a subpoena to compel production of any documents.

Petitioner's theory about subpoenas for private papers thus requires this Court to resolve a hypothetical scenario about subpoenas never filed for documents never compelled. "Because of [the] traditional reluctance to extend constitutional interpretations to situations or facts which are not before the Court," Petitioner's argument "is unnecessary to [the case's] disposition." *Sweatt v. Painter*, 339 U.S. 629, 631 (1950).

2. Petitioner's proposed rule does not support reversal of the judgment below.

Even if Petitioner's argument were properly before the Court, it would not help her on the facts of this case for two reasons. First, Petitioner's own common law analysis does not extend the privilege to cases like this one, where the State has the evidence. Cases like *King v. Purnell* (1748) 96 Eng. Rep. 20, stand for the limited proposition that the person who is actually in possession of documents cannot be compelled to produce them if they are incriminating. *See also Roe v. Harvey* (1769) 98 Eng. Rep. 302, 305 (noting that defendant may not be

[11] Petitioner suggests that her argument would become relevant if the government compelled her to enter the passwords into the devices. Pet'r's Br. 37 n.1. Since the government would still control the devices, compelled password entry would no more "produce" the documents than Doe's signature produced the bank records in *Doe II*.

forced to produce evidence that he "hold[s] . . . in his hands"); Richard A. Nagareda, *Compulsion "To Be a Witness" and the Resurrection of* Boyd, 74 N.Y.U. L. Rev. 1575, 1620–21 (1999). Here, the government has already taken the evidence out of Petitioner's hands. *See* Nagareda, *supra*, at 1623 (distinguishing between suspect giving and government taking evidence).

Second, Petitioner cannot establish that the device's contents are private documents. Cell phones and computers may contain data that the user actively generates like videos and texts in addition to data that the device passively generates about the user's calls, texts, internet browsing, and location. *See Riley*, 573 U.S. at 393, 395–96. User-created media bear a passing resemblance to private documents like diaries. Data that the device creates to track the user do not. And unlike private documents, phone data are sometimes shared with third parties without user knowledge. *Cf. Carpenter*, 138 S. Ct. at 2216–17 (involving cell phone location records). A rule privileging private documents should not be innovated in a case where the record does not establish whether the data at stake are private documents.

CONCLUSION

For the foregoing reasons, the judgment of the Ames Supreme Court should be affirmed.

February 19, 2021

Respectfully submitted,

The Lloyd L. Gaines Memorial Team

/s/ Jason Bell

/s/ Ameze Belo-Osagie

/s/ Lauren Bilow

/s/ Davis Campbell

/s/ Travis Fife

/s/ Michael Torcello

APPENDIX

U.S. Const. amend. I provides:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

U.S. Const. amend. V provides:

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

The Nonconsensual Pornography Act, Ames Crim. Stat. 545, provides:

> (a) Legislative findings and purpose.
>
> (1) The disclosure of private sexual images and videos without the consent of the subjects of those images and videos is a major social problem requiring immediate legislative response.
>
> (2) Freedom of speech is a prized value, but the nonconsensual disclosure of private sexual images and videos constitutes an egregious breach of privacy, and is speech of essentially no value to society.
>
> (3) The nonconsensual disclosure of private sexual images and videos often results in severe harm to the subjects, including but not limited to loss of professional opportunities and reputation, harassment and threats, and severe emotional distress.

(4) These harms are likely to occur regardless of the knowledge, intentions, or motivations of the person who discloses a private sexual image or video.

(5) Once images and videos are disclosed—and especially once they make their way to the Internet—they are likely to proliferate beyond control, and to remain in the public domain indefinitely, where they will continue to cause harm. Thus, it is imperative to deter and prevent the nonconsensual disclosure of private sexual images and videos before it occurs.

(6) Existing legal remedies are inadequate to deter and prevent the nonconsensual disclosure of private sexual images and videos.

(b) Definitions. For the purposes of this Section:

(1) "Disclose" includes transferring, publishing, distributing, or reproducing an image so that it may be seen by at least one other person;

(2) "Image" includes a photograph, film, videotape, recording, digital, or other reproduction;

(3) "Intimate parts" means the naked genitals, pubic area, anus, or female post-pubescent nipple of the person;

(4) "Sexual act" includes but is not limited to masturbation; genital, anal, or oral sex; sexual penetration with objects; or the transfer or transmission of semen upon any part of the depicted person's body.

(c) A person may not knowingly disclose an image of another, identifiable person whose intimate parts are exposed or who is engaged in a sexual act, if the person making the disclosure knows or should know that the person depicted reasonably expected that the image would remain private, and knows or should know that the person depicted did not consent to such disclosure.

(d) The following activities are exempt from the provisions of this Section:

(1) Images involving voluntary exposure in public or commercial settings;

(2) Disclosures made to a small audience to advance the public interest, including but not limited to the reporting of unlawful conduct to competent authorities, or the lawful and common practices of law enforcement, criminal reporting, legal proceedings, or medical treatment.

(e) Nothing in this Section shall be construed to impose liability upon the following entities solely as a result of content or information provided by another person:

(1) an interactive computer service, as defined in 47 U.S.C. 230(f)(2);

(2) a telecommunications network or broadband provider.

(f) Sentence. Disclosure of images in violation of this statute is a Class C misdemeanor punishable by up to 6 months in jail and/or a fine of $2000.

(g) Severability. The provisions of this statute are severable. If any is deemed to be unconstitutional or otherwise contrary to law, the intent of the legislature is that the remainder of the statute remain in effect.

Supreme Court Rule 14 provides in relevant part:

1. A petition for a writ of certiorari shall contain, in the order indicated:

(a) The questions presented for review, expressed concisely in relation to the circumstances of the case, without unnecessary detail. The questions should be short and should not be argumentative or repetitive. If the petitioner or respondent is under a death sentence that may be affected by the disposition of the petition, the notation "capital case" shall precede the questions presented. The questions shall be set out on the first page following the cover, and no other information may appear on that page. The statement of any question presented is deemed to comprise every subsidiary question fairly included therein. Only the questions set out in the petition, or fairly included therein, will be considered by the Court.